SHILCreateFromPath

Vulnerable to TOCTOU issues

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-16

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 5841 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Path spoofing or confusion problem</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Indeterminate File/Path
• TOCTOU - Time of Check, Time of Use</td></tr>
<tr><td><b>Software Context</b></td><td>• File Management</td></tr>
<tr><td><b>Location</b></td><td></td></tr>
<tr><td><b>Description</b></td><td>Creates a pointer to an item identifier list (PIDL) from a path.
SHILCreateFromPath is vulnerable to TOCTOU attacks.</td></tr>
<tr><td><b>APIs</b></td><td><table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>SHILCreateFromPath</td><td>use</td></tr></table></td></tr>
<tr><td><b>Method of Attack</b></td><td>The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results.</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td>Generally applicable.</td><td>Utilize a file descriptor version of stat/ fstat when checking.</td><td>Effective.</td></tr><tr><td>Generally applicable.</td><td>The most basic advice for TOCTOU vulnerabilities</td><td>Does not resolve the underlying vulnerability</td></tr></table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

		is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help to limit the false sense of security given by the check. Attempt to create the directory and then check status after the creation.	but limits the false sense of security given by the check.
	Generally applicable.	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Recheck the resource after the use call to verify that the action was taken appropriately.	Effective in some cases.
Signature Details	HRESULT SHILCreateFromPath (LPCWSTR pszPath, LPITEMIDLIST *ppidl, DWORD *rgflnOut		

<table>
<tr><td></td><td>);</td></tr>
<tr><td><b>Examples of Incorrect Code</b></td><td><code>int use_status;
struct stat statbuf;
Pidl: PItemIDList;
Attributes: ULONG;

check_status=stat("the_path", &statbuf);

[...]

SHILCreatefromPath("the_path", Addr(Pidl), Attributes);</code></td></tr>
<tr><td><b>Examples of Corrected Code</b></td><td><code>[...]

Pidl: PItemIDList;
Attributes: ULONG;

SHILCreatefromPath("the_path", Addr(Pidl), Attributes);

[...]</code></td></tr>
<tr><td><b>Source References</b></td><td>• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shilcreatefrompath.asp[2]
• http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shilcreatefrompath.asp[3]</td></tr>
<tr><td><b>Recommended Resource</b></td><td></td></tr>
<tr><td><b>Discriminant Set</b></td><td><table><tr><td><b>Operating System</b></td><td>• Windows</td></tr><tr><td><b>Languages</b></td><td>• C
• C++</td></tr></table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com